

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

1/5/1 (Item 1 from file: 351).
DIALOG(R) File 351:Derwent WPI
(c) 2001 Derwent Info Ltd. All rts. reserv.

010893224 **Image available**
WPI Acc No: 1996-390175/199639
XRPX Acc No: N96-328738

Code algorithm intensity evaluation for e.g. finite element analysis,
data encryption standard - involves extracting search pattern and
computing of required data content for code decipherment through linear
decipherment method

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 8190344	A	19960723	JP 952872	A	19950111	199639 B

Priority Applications (No Type Date): JP 952872 A 19950111

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 8190344	A	17	G09C-001/00	

Abstract (Basic): JP 8190344 A

The method involves extracting a pattern candidate from a
constraint using a search pattern extractor (120). An initial value
setting (110) is provided during the search for the factor of the max.
variation of a stage linear expression. A best-expression searcher
(130) seeks for the stage linear expression for the search pattern
assembly.

An data-content calculator (140) computes the required max.
variation factor for code decipherment through linear decipherment
method. A result output unit (150) displays the computed data content.

ADVANTAGE - Ensures accelerated search for best expression.

Dwg.2/11

Title Terms: CODE; ALGORITHM; INTENSITY; EVALUATE; FINITE; ELEMENT; ANALYSE
; DATA; ENCRYPTION; STANDARD; EXTRACT; SEARCH; PATTERN; COMPUTATION;

REQUIRE; DATA; CONTENT; CODE; THROUGH; LINEAR; METHOD

Index Terms/Additional Words: FEA; DES

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00

International Patent Class (Additional): H04L-009/00; H04L-009/10;
H04L-009/12

File Segment: EPI; EngPI

1/5/2 (Item 1 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2000 JPO & JAPIO. All rts. reserv.

05234844 **Image available**
EVALUATION METHOD FOR STRENGTH OF CIPHER ALGORITHM AND STRENGTH EVALUATION
DEVICE

PUB. NO.: 08-190344 JP 8190344 A]

PUBLISHED: July 23, 1996 (19960723)

INVENTOR(s): ARAKI SHIHO

OTA KAZUO

AOKI KAZUMARO

APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese
Company or Corporation), JP (Japan)

APPL. NO.: 07-002872 [JP 952872]

FILED: January 11, 1995 (19950111)

INTL CLASS: [6] G09C-001/00; H04L-009/00; H04L-009/10; H04L-009/12

JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION --
Telegraphy)

ABSTRACT

PURPOSE: To provide an evaluation method for strength of cipher algorithm
and a strength evaluation device which are adaptable to an involution type

cipher such as FEAL and the like which have more search calculation quantity than DES in a practical time.

CONSTITUTION: This device has an initial value setting means 110 setting an initial value when the maximum deviation rate of (n) stages linear expression of a cipher algorithm is searched, a search candidate extracting means 120 extracting a search pattern candidate conforming to a restriction condition, a best expression search means 130 searching n stages linear expression of the maximum deviation rate for search pattern candidate assemblage, a non-cipher information quantity calculating means 140 calculating non-cipher information quantity required for performing cipher decoding by a linear decoding method from the maximum deviation rate, and an output means 150 outputting non-cipher information quantity.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-190344 ✓

(43) 公開日 平成8年(1996)7月23日

(51) Int.Cl.⁶

G 0 9 C 1/00

H 0 4 L 9/00

9/10

9/12

識別記号

庁内整理番号

7259-5J

F I

技術表示箇所

H 0 4 L 9/00

Z

審査請求 未請求 請求項の数 4 O L (全 17 頁)

(21) 出願番号

特願平7-2872

(22) 出願日

平成7年(1995)1月11日

(71) 出願人 000004228

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 荒木 志帆

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 太田 和夫

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 青木 和麻呂

千葉県我孫子市並木5-6-37

(74) 代理人 弁理士 伊東 忠彦

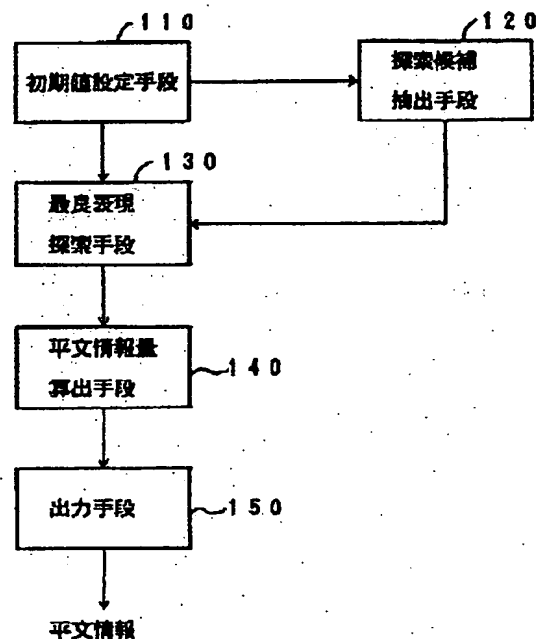
(54) 【発明の名称】 暗号アルゴリズムの強度評価方法及び強度評価装置

(57) 【要約】

【目的】 本発明の目的は、DESよりも探索計算量が多いFEAL等のinvolution型暗号への実用的な時間で適用可能な暗号アルゴリズムの強度評価方法及び強度評価装置を提供することである。

【構成】 本発明は、暗号アルゴリズムのn段線形表現の最大偏差率を探索する際の初期値を設定する初期値設定手段110と、制約条件から探索パターン候補を抽出する探索候補抽出手段120と、探索パターン候補集合を対象に、偏差率最大のn段線形表現を探索する最良表現探索手段130と、最大偏差率より線形解読法により暗号解読を行うのに必要な平文情報量を算出する平文情報量算出手段140と、平文情報量を出力する出力手段150とを有する。

本発明の原理構成図



【特許請求の範囲】

【請求項1】 インボルーション (involution) 型暗号アルゴリズムを排他的論理和演算を用いて線形近似した式のうち、偏差率最大で成り立つ線形近似式を探索することにより、その暗号アルゴリズムの強度を評価する暗号アルゴリズムの強度評価方法において、

探索に先立って各段の f 関数の線形表現の偏差率に関する制約条件から探索候補集合を絞っておき、前記探索候補集合の要素に対してのみ探索を行うことを特徴とする暗号アルゴリズムの強度評価方法。

【請求項2】 探索集合を決定する第1の条件として、 n をある自然数とし、 n 段最良表現を探索するとき、 n 段線形表現に含まれる全ての r (r は、 $r < n$ を満たす自然数) 段線形表現について、その偏差率が既知の r 段線形表現の最大偏差率を越えるものは探索しない、及び第2の条件として、どの n 段最良表現の探索候補についても

【数1】

$$1 \leq i \leq \lfloor n/2 \rfloor$$

を満たす全ての自然数 i について i 段 f 関数の線形表現と $n-1+1$ 段 f 関数の線形表現を入れ換えた候補が存在するが、探索計算量の少ない方のみを対象とするという2つの制約条件により前記探索候補集合を絞る請求項1記載の暗号アルゴリズムの強度評価方法。

【請求項3】 インボルーション (involution) 型暗号アルゴリズムを排他的論理和演算を用いて線形近似した式のうち、偏差率最大で成り立つ線形近似式を探索することにより、該暗号アルゴリズムの強度を評価する機能を有する暗号化アルゴリズムの強度評価装置において、前記暗号アルゴリズムの n (n は自然数) 段線形表現の最大偏差率を探索する際の初期値を設定する初期値設定手段と、

各段の f 関数の線形表現の偏差率に関する制約条件から探索候補を抽出する探索候補抽出手段と、

前記探索候補抽出手段から抽出された探索候補集合を対象に、偏差率最大の n 段線形表現を探索する最良表現探索手段と、

前記最良表現探索手段から出力された最大偏差率より、線形解読法により暗号解読を行うのに必要な平文情報量を算出する平文情報量算出手段と、

前記平文情報量算出手段で算出された前記平文情報量を出力する出力手段とを有することを特徴とする強度評価装置。

* 【請求項4】 前記探索候補抽出手段は、

各段の f 関数の偏差率を定めた探索パターン候補を設定する探索パターン候補設定手段と、

前記探索パターン候補設定手段により設定された前記探索パターン候補のうち、最良偏差率の初期値を満たさない探索パターンは棄却する第1のチェック手段と、

n をある自然数とし、 n 段最良表現を探索するとき、 n 段線形表現に含まれる全ての r (r は、 $r < n$ を満たす自然数) 段線形表現について、その偏差率が既知の r 段線形表現の最大偏差率を越えるものは探索しないという条件を満たすかをチェックする第2のチェック手段と、どの n 段最良表現の探索候補についても

【数2】

$$1 \leq i \leq \lfloor n/2 \rfloor$$

を満たす全ての自然数 i について i 段 f 関数の線形表現と $n-1+1$ 段 f 関数の線形表現を入れ換えた候補が存在する場合に、探索計算量の少ない方のみを対象とするチェックを行う第3のチェック手段とを含む請求項3記載の強度評価装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、暗号アルゴリズムの強度評価方法及び強度評価装置に係り、特に、仕様が公開された暗号アルゴリズムに対して、その暗号アルゴリズムから構成し得る最大の偏差率をもつ線形近似式を探索し、この結果から暗号アルゴリズムの線形解読法に対する強度を定量的に評価することが可能な暗号アルゴリズムの強度評価方法及び強度評価装置に関する。

【0002】

【従来の技術】 近年、ブロック暗号に対する有力な既知平文攻撃法として、線形解読法が注目されている (詳細は、松井充「DES暗号の線形解読法(1)」、SCIS 93-3C, (Jan, 1993) を参照のこと)。既知平文攻撃とは、暗号攻撃者が何等からの手段で入手した暗号文に対してその平文を入手できる状況下において、この暗号文—平文の対から暗号鍵を解くことである。線形解読法の原理はランダムに与えられた平文 P と対応する暗号文 C 、及び暗号化鍵 K に対して有意な確率 P ($\neq 1/2$) で成立する。以下の式(1)で表されるような線形近似式を構成し、最尤法を用いて暗号化鍵の K (k_1, k_2, \dots, k_c) (1 bit) を推定することである。

【0003】

$$P[i_1, i_2, \dots, i_a] \oplus C[j_1, j_2, \dots, j_b] = K[k_1, k_2, \dots, k_c] \quad \text{with probability } P \quad \dots (1)$$

$[i_1, i_2, \dots, i_a]$, $[j_1, j_2, \dots, j_b]$, $[k_1, k_2, \dots, k_c]$ は固定されたビット位置を示す。但し、“ \oplus ” は、XOR (排他的論理和) 演算を表す。

【0004】 $A[i, j, \dots, k] = A[i] \oplus A$

$[j] \oplus \dots \oplus A[k]$

また、 $[i_1, i_2, \dots, i_a]$, $[j_1, j_2, \dots, j_b]$, $[k_1, k_2, \dots, k_c]$ の代わりにマスク値 ΓP , ΓC , ΓK を用いて以下の式(2)のように書き換えることができる。

【0005】

$$P[\Gamma P] \odot C[\Gamma C] = K[\Gamma K] \text{ with probability } P \quad \dots (2)$$

但し、

$$A[\Gamma X] = \bigoplus_{i=1}^n a_i x_i, \quad A = (a_1, \dots, a_n), \quad \Gamma X = (x_1, \dots, x_n), \quad a_i, x_i \in \{0, 1\}$$

線形解読法では、解読に必要な平文情報量Nは解読に用いる線形近似式の偏差率P'から

$$N = c \times P'^{-2}$$

の式を用いて算出できる。線形近似式の偏差率P'は、

$$P' \stackrel{\text{def}}{=} |P - 1/2|$$

で定義され、cは暗号アルゴリズムに依存して決まる定数である。暗号攻撃者は攻撃対象の暗号アルゴリズムから構成し得る式(1)の線形近似式のうち、偏差率最大の近似式(以下、最良近似式、または、最良表現と呼ぶ)を見つけることにより、最小の平文情報量で解読が可能となる。

【0006】まず、式(1)で表される一般の線形近似*

$$I_1[\Gamma I_1] \odot O_1[\Gamma O_1] = K_1[\Gamma K_1] \text{ with probability } p_1(\Gamma O_1, \Gamma I_1) \quad \dots (3)$$

このf関数の線形近似式の偏差率p' (ΓO₁, ΓI₁)は以下の式(4)で与えられる。 ※ 【0008】

$$p'(\Gamma O_1, \Gamma I_1) = |p_1(\Gamma O_1, \Gamma I_1) - 1/2| \quad \dots (4)$$

【0009】involution型暗号アルゴリズムに含まれるXOR(排他的論理和)演算⊕やブランチ(BRANCH)演算#において、マスク値の演算は、以下の式のように行われる。マスク値の関係を図8に示す。但し、X, Y, Zはデータを、ΓX, ΓY, ΓZは、X, Y, Zへのマスク値である。

【0010】XOR演算⊕において、X=Y⊕Zが成り立つとき、

$$\Gamma O_i = \Gamma O_{i-2} \odot \Gamma I_{i-1} \quad (3 \leq i \leq n) \quad \dots (5)$$

ここで、式(5)の関係を満たすように、各i段(1 ≤ i ≤ n)のf関数の線形近似式の(ΓO_i, ΓI_i) (1 ≤ i ≤ n)を決める。ここで、決定されたn個のf関数の線形近似式(3)より式(1)の線形近似式が求められる。 ☆

$$P' = 2^{n-1} \prod_{i=1}^n (p'(\Gamma O_i, \Gamma I_i)) \quad \dots (6)$$

【0014】各i段のf関数の線形表現(ΓO_i, ΓI_i)からマスク値に関する演算規則(5)を用いて式(1)を導く具体例として3段DESの場合を図9を用いて説明する。1, 2, 3段目f関数についてそれぞれ次の線形近似式が成り立つ。

$$O_1[7, 18, 24, 29] = I_1[15] \odot K$$

$$I_1[22] \text{ with probability } p_1 = 12/64$$

$$O_2[\] = I_2[\] \odot K_2[\] \text{ with probability } p_2 = 1$$

$$O_3[7, 18, 24, 29] = I_3[15] \odot K$$

*式の構成方法を以下に述べる。図7は、一般のインボルーション(involution)型暗号アルゴリズムの説明図である。同図に示す一般のn段のinvolution型暗号を用いて説明する。involution型暗号の例として、DES(詳細は、"Data Encryption Standard," Federal Information Processing Standards Publication 46, National Bureau of Standards, U.S. Department of Commerce, 1977を参照のこと)、FEAL(詳細は宮口、栗原、太田、森田「FEAL暗号の拡張」NTT, R&D, Vol. 39, No.10, pp.1439-1450, 1990 参照のこと)などがある。i段目のf関数の入力値をI_i、出力値をO_i、鍵をK_i、入力値、出力値、鍵に対するマスク値をそれぞれΓI_i、ΓO_i、ΓK_iとすると、i段目のf関数の線形近似式は式(3)のように表される。

【0007】

★ΓX=ΓY=ΓZ,

ブランチ演算#において、X#(Y, Z), X=Y=Zが成り立つとき、

$$\Gamma X = \Gamma Y \odot \Gamma Z$$

となり、これより、i-1, i, i+1段の入出力マスク値の間に成り立つ関係式(5)が導かれる。

【0011】

☆【0012】この線形近似式の偏差率P'は式(6)で与えられる。

【0013】

【数4】

$$s[22] \text{ with probability } p_3 = 12/64$$

これらの式にI₁=P_L, I₃=C_L, I₂=P_H⊕O₁=C_H⊕O₃を適用して次式を得る。

$$[0015] P_H[7, 18, 24, 29] \odot C_H[7, 18, 24, 29]$$

$$\odot P_L[15] \odot C_L[15] = K_1[22] \odot K$$

$$s[22]$$

この近似式が成り立つ偏差率P'は、

$$P' = 2^{3-1} (20/63 \times 1/2 \times 20/63) =$$

$$50 \quad 0.195$$

次に、最良近似式の探索方法について述べる。まず、
「最良近似式」の定義について述べる。n段の暗号アル
ゴリズムの最良近似式の偏差率をBEST_nと書くこと
にし、n段最良偏差率と呼ぶ。これを式(7)で定義す*

する。

[0016]

[数5]

$$BEST_n =$$

$$\Gamma O_i = \max_{\Gamma O_{i-2} \leq \Gamma I_{i-1} \ (3 \leq i \leq n) \ \Gamma P \neq 0}$$

$$(2^{i-1} \prod_{j=1}^i (p'(\Gamma O_j, \Gamma I_j))) \quad (7)$$

[0017] 即ち、各マスク値間で式(5)を満たし、
かつn段分つなげた時の全体の偏差率が最大となるよう
にi段目の線形表現($\Gamma O_i, \Gamma I_i$)を決定すること
により得られる線形近似式を最良近似式とする(但し、
 $1 \leq i \leq n$)。最良近似式表現の探索アルゴリズムにつ
いては、“時田、反町、松井「線形解読法における最良
表現の効率的な探索アルゴリズム」、電子情報通信学会
技術研究報告ISEC93-97, (Mar, 1994)”にお
いて提案されており、DES型のS-boxを持つ暗号ア※

※ルゴリズムに対する適用結果が記されている。この探索
アルゴリズムは、以下に示す再帰的ルーチンにより表さ
れる。但し、 $\neg BEST_n$ は、BEST_nの初期値であ
り、 $r < n$ なる全ての自然数rについて、BEST_rは
既知でなければならない。また、 $[p'_1, p'_2, \dots, p'_i]$ は、式(8)で表される値とする。

[0018]

[数6]

$$[p'_1, p'_2, \dots, p'_i] = 2^{i-1} \prod_{j=1}^i p'_j \quad (8)$$

[0019] ここで、involution型暗号の最良表現探索
アルゴリズム(Procedure Best Search (n, $\neg BEST_n$))
について説明する。

★入力 n: 求める線形表現の段数

$\neg BEST_n$: n段の最良偏差率の初期値

★出力 BEST_n: n段最良偏差率

Procedure Round-1: (1段目f関数の線形表現を決定する)

For each candidate for ΓO_1 , do the following:

† Let $p'_1 = \max \Gamma I p'_1 (\Gamma O_1, \Gamma I)$.

† If $[p'_1, BEST_{n-1}] < \neg BEST_n$, then try another
candidate for ΓO_1 .

† Call Procedure Round-2.

BEST_n = $\neg BEST_n$.

Print BEST_n.

Exit the program.

Procedure Round-2: (2段目f関数の線形表現を決定する)

For each candidate for ΓO_2 and ΓI_2 , do the following:

† Let $p'_2 = p'_2 (\Gamma O_2, \Gamma I_2)$.

† If $[p'_1, p'_2, BEST_{n-2}] < \neg BEST_n$, then try another
candidate for ΓO_2 and ΓI_2 .

† Call Procedure Round-3.

Return to the upper procedure.

Procedure Round-i ($3 \leq i \leq n-1$) (i段目f関数の線形表現を決定する)

For each candidate for ΓI_i , do the following:

† Let $\Gamma O_i = \Gamma O_{i-2} \odot \Gamma I_{i-1}$.

† Let $p'_i = p'_i (\Gamma O_i, \Gamma I_i)$.

† If $[p'_1, p'_2, \dots, p'_i, BEST_{n-i}] < \neg BEST_n$,
then try another candidate for ΓI_i .

† Call Procedure Round-(i+1).

Return to the upper procedure.

Procedure Round-n: (n 段目 f 関数の線形表現を決定する)

† Let $\Gamma O_n = \Gamma O_{n-2} \odot \Gamma I_{n-1}$.

† Let $p'_n = \max \Gamma I p'_n (\Gamma O_n, \Gamma I)$.

† If $[p'_1, p'_2, \dots, p'_n] > \neg BEST_n$, then $\neg BEST_n$,
 $= [p'_1, p'_2, \dots, p'_n]$.

Return to the upper procedure.

ΓO_1 や ΓI_1 の候補の与え方は、暗号アルゴリズムに依存するものであるし、その与え方も任意であるが、

p' ($\Gamma O_1, \Gamma I_1$) の値の大きい順に並べたリストを格納しておき、 ΓO_1 や ΓI_1 を与える装置を用意することで計算量が削減できる。

$[p'_1, p'_2, \dots, p'_1, BEST_{n-1}] \geq \neg BEST_n \dots (9)$

式 (9) を式 (8) を用いて変形すると、以下の式のようになる。

$$p'_i \geq \frac{\neg BEST_n}{2^i \times p'_1 \times \dots \times p'_{i-1} \times BEST_{n-1}}$$

【0022】 p'_i ($1 \leq i \leq n$) の探索範囲が式 (10) で決定することより、上記の従来の方法では、以下のような問題が存在する。今、n 段最良表現の探索を行っており、Procedure Round-n まで探索が進んだとする。この時 $p'_1 = q'_1, p'_2 = q'_2, \dots, p'_n = q'_n$ であるとき、探索パターンを $(q'_1, q'_2, \dots, q'_n)$ と書くことにする。

$$\begin{aligned} [q'_1, q'_2, \dots, q'_n] &\leq \neg BEST_n \\ [q'_2, q'_3, \dots, q'_n] &\leq BEST_{n-1} \\ [q'_3, q'_4, \dots, q'_n] &\leq BEST_{n-2} \end{aligned}$$

これらの条件は「n 段目を含む r ($1 \leq r \leq n$) 段線形表現の偏差率はそれぞれ r 段最良表現の偏差率 $BEST_r$ 以下の値をとる」という条件であり、「n 段線形表現に含まれる全ての r ($1 \leq r \leq n$) 段線形表現の偏差率はそれぞれ r 段の最良表現の偏差率 $BEST_r$ 以下の値をとる」が必ずしも満たされていない。即ち、従来の方法では、

$$[q'_1, q'_{i+1}, \dots, q'_{i+r-1}] > BEST_r$$

($1 \leq i \leq n, i+r-1 \leq n$) となる探索パターンについて探索対象としてしまう場合がある。 $BEST_r$ の定義より上記の式を満たす探索パターンは、図 10 に示すように、明らかに不要な探索である。

【0025】問題点 2. 同じ探索パターンの重複探索：暗号文を暗号化鍵を用いて解読して元の平文に戻ることにより、平文 P と暗号文 C の役目を入れ換えてもよく。式 (1) は、 P と C 、 ΓP と ΓC を入れ換えても成り立つ。即ち、n 段線形表現の全ての i ($1 \leq i \leq n$) について i 段目の f 関数線形表現 ($\Gamma O_i, \Gamma I_i$) を $n-i+1$ 段目の f 関数線形表現 ($\Gamma O_{n-i+1}, \Gamma I_{n-i+1}$) と入れ換えたものからも同じ n 段線形表現が

* 【0020】

【発明が解決しようとする課題】従来の n 段最良表現の探索方法においては、 i (i は $1 \leq i \leq n$ を満たす自然数) 段目において式 (9) に示す制約条件を満たす偏差率 p'_i を持つ f 関数の線形表現の探索を行う。

* 【0021】

【数 7】

★ 【0023】問題点 1. 不要な探索パターンの探索：従来のアルゴリズムでは、探索パターン $(q'_1, q'_2, \dots, q'_n)$ について図 10 に示すように式 (10) から導かれる以下の状態のみしか満たされていない。

【0024】

$$[q'_n] \leq BEST_1 \quad (11)$$

構成できる。ところで、従来の方法では、どちらか片方のみの探索で十分であるにもかかわらず、式 (9) の条件を満たす探索パターン $(q'_1, q'_2, \dots, q'_n)$ と探索パターン $(q'_n, q'_{n-1}, \dots, q'_1)$ の両方について、図 11 に示すように重複探索が行われている。

【0026】このように、従来の方法では、段数が増えるに従い、探索候補数が指数関数的に増加し、現実的な実行時間で最良の表現を求められない場合が生じる。本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、DES よりも探索計算量が多い FEA L 等の involution 型暗号への実用的な時間で適用可能な暗号アルゴリズムの強度評価方法及び強度評価装置を提供することを目的とする。

【0027】

【課題を解決するための手段】図 1 は、本発明の原理を説明するための図である。本発明は、インボルーション (involution) 型暗号アルゴリズムを排他的論理和演算を用いて線形近似した式のうち、偏差率最大で成り立つ線形近似式を探索することにより、その暗号アルゴリズムの強度を評価する暗号アルゴリズムの強度評価方法にお

いて、探索に先立って各段の f 関数の線形表現の偏差率に関する制約条件から探索候補集合を絞っておき（ステップ1）、探索候補集合の要素に対してのみ探索を行う（ステップ2）。

【0028】また、探索集合を決定する第1の条件として、 n をある自然数とし、 n 段最良表現を探索するとき、 n 段線形表現に含まれる全ての r (r は、 $r < n$ を満たす自然数) 段線形表現について、その偏差率が既知の r 段線形表現の最大偏差率を超えるものは探索しない、及び第2の条件として、どの n 段最良表現の探索候補についても

【0029】

【数8】

$$1 \leq i \leq \lfloor n/2 \rfloor$$

【0030】を満たす全ての自然数 i について i 段 f 関数の線形表現と $n-1+1$ 段 f 関数の線形表現を入れ換えた候補が存在するが、探索計算量の少ない方のみを対象とするという2つの制約条件により探索候補集合を絞る。図2は、本発明の原理構成図である。

【0031】本発明は、インボルーション (involution) 型暗号アルゴリズムを排他的論理和演算を用いて線形近似した式のうち、偏差率最大で成り立つ線形近似式を探索することにより、該暗号アルゴリズムの強度を評価する機能を有する暗号化アルゴリズムの強度評価装置において、暗号アルゴリズムの n (n は自然数) 段線形表現の最大偏差率を探索する際の初期値を設定する初期値設定手段110と、各段の f 関数の線形表現の偏差率に関する制約条件から探索パターン候補を抽出する探索候補抽出手段120と、探索候補抽出手段120から抽出された探索パターン候補集合を対象に、偏差率最大の n 段線形表現を探索する最良表現探索手段130と、最良表現探索手段130から出力された最大偏差率より線形解読法により暗号解読を行うのに必要な平文情報量を算出する平文情報量算出手段140と、平文情報量算出手段140で算出された平文情報量を出力する出力手段150とを有する。

【0032】また、上記の探索候補抽出手段120は、各段の f 関数の偏差率を定めた探索パターン候補を設定する探索パターン候補設定手段と、探索パターン候補設定手段により設定された探索パターン候補のうち、最良偏差率の初期値を満たさない探索パターンは棄却する第1のチェック手段と、 n をある自然数とし、 n 段最良表現を探索するとき、 n 段線形表現に含まれる全ての r (r は、 $r < n$ を満たす自然数) 段線形表現について、その偏差率が既知の r 段線形表現の最大偏差率を超えるものは探索しないという条件を満たすかをチェックする第2のチェック手段と、どの n 段最良表現の探索候補についても

【0033】

【数9】

$$1 \leq i \leq \lfloor n/2 \rfloor$$

【0034】を満たす全ての自然数 i について i 段 f 関数の線形表現と $n-1+1$ 段 f 関数の線形表現を入れ換えた候補が存在するが、探索計算量の少ない方のみを対象とするチェックを行う第3のチェック手段とを含む。

【0035】

【作用】本発明は、各段の f 関数線形表現の偏差率を探索に先立って算出しておき、各段の f 関数線形表現の偏差率に関する制約条件を満たす探索パターン (p'_1, p'_2, \dots, p'_n) を全て抽出する装置を付加し、以下で述べる2つの条件により不要な探索候補や、重複探索を削除する。この装置により抽出される全ての探索パターンを「探索パターン集合」と呼ぶことにすると、この抽出されたパターン集合の要素全てについて、従来の探索アルゴリズムに変更を加えた探索アルゴリズムを適用して、探索を行えばよい。

【0036】探索パターン抽出装置は、下の2つの条件を満たす探索パターン (q'_1, q'_2, \dots, q'_n) を出力する機能をもつ。

・条件1：不要な探索パターンの削除

$1 \leq i \leq n, i+r-1 \leq n$ を満たす全ての i, r に対して以下の式を満たすこと。

$$[q'_1, q'_{i+1}, \dots, q'_{i+r+1}] \leq \text{BEST}$$

・条件2：重複探索の防止

探索パターン (p'_1, p'_2, \dots, p'_n) の探索に必要な計算量を $C(p'_1, p'_2, \dots, p'_n)$ と定義すると、以下の式を満たすこと。

$$C(q'_1, q'_2, \dots, q'_n) \leq C(q'_n, q'_{n-1}, \dots, q'_1)$$

探索パターン (p'_1, p'_2, \dots, p'_n) の探索に必要な計算量の比較は、探索候補数を比較することで行う。しかし、探索候補数を正確に計算するには、最良表現探索と同様の計算量が必要である。しかし、本発明で提案する探索アルゴリズムを用いた最良表現探索では、探索全体の探索候補数が2段目までの探索候補数と同じオーダー (order) であることがわかっているので、2段目までの探索候補数を計算することで見積もることができる。この計算式は暗号アルゴリズムに依存するが、 p'_1, p'_2 をパラメータとする関数で計算できる。

【0037】従来は、段数が増えるに従い、探索候補数が指数関数的に増加し、現実的な実行時間で最良表現を求められない場合が生じるが、本発明は、暗号アルゴリズムの各段の f 関数線形表現の偏差率のみに関する制約条件により、 f 関数線形表現 (FO_1, FI_1) の決定とは独立に解決可能である。

【0038】

【実施例】以下、図面と共に本発明の実施例を説明する。図3は、本発明の一実施例の強度評価装置の構成を示す。同図に示す強度評価装置は、暗号アルゴリズムの

n (n は自然数) 段線形表現の最大偏差率を探索する際の初期値を設定する初期設定装置110、各段の f 関数の線形表現の偏差率に関する制約条件から探索すべき候補を抽出する探索パターン抽出装置120、抽出された探索候補集合を対象に、偏差率最大の n 段線形表現を探索する最良表現探索装置130、最良表現探索装置130から出力された最大偏差率より線形解読法により暗号解読を行うために必要な平文情報量を算出する必要平文情報量計算装置140、算出された平文情報量を出力する結果出力装置150、探索パターン集合160、結果ファイル170及び結果プリント180より構成される。

【0039】図4は、本発明の一実施例の暗号アルゴリズムの強度評価方法の概要を示すフローチャートである。上記の図3と共に以下に強度評価方法の動作を説明*

[Pattern₁, Pattern₂, ..., Pattern _{$\phi(n, \neg \text{BEST}_n)$}]

【0042】を決定する。但し、 $\phi(n, P')$ は偏差率 P' の n 段線形表現の探索パターン集合の要素数である。手続きExtract($n, \neg \text{BEST}_n$)に関する詳細な構成及び動作は、図5、6に後述する。

【0043】ステップ103) 探索パターン抽出装置120から出力された探索パターンすべてについて最良表現探索装置130(フローチャート中の手続き名はSearch($n, \text{Pattern}_i$))を用いて、Pattern _{i} ($P'_{11}, P'_{12}, \dots, P'_{1n}$)について線形表現の探索を行う。手続きSearch($n, \text{Pattern}_i$)のアルゴリズムは後述する。

【0044】ステップ104) 全ての i について、 $[P'_{11}, P'_{12}, \dots, P'_{1n}] = \neg \text{BEST}_n$ を満たす線形表現が存在するか否かを判定し、存在する場合にはステップ106に移行し、存在しない場合にはステップ105に移行する。

【0045】ステップ105) 上記の式を満たす線形表現が存在しない場合には、初期値設定装置110で、 $\neg \text{BEST}_n = \neg \text{BEST}_n \times \alpha$ と設定し直し、ステップ102に移行する。上記の式で α は、 $0 < \alpha \leq 1$ を満たす定数で、暗号アルゴリズムにより適切な値を選択できる。例えば、FEAL暗号の場合には、 $\alpha = 1/2$ である。

【0046】ステップ106) $[P'_{11}, P'_{12}, \dots, P'_{1n}] = \neg \text{BEST}_n$ を満たす線形表現が存在すれば、最良表現探索装置130は、この値 $\neg \text{BEST}_n$ を最良偏差率 BEST_n として出力する。

ステップ107) 必要平文情報量計算装置140を用いて、その暗号アルゴリズムの線形解読に必要な平文情報量 N を算出する。この装置は、具体的には、 $N = c \times (\neg \text{BEST}_n)^{-2}$

を計算する乗算回路で実現できる。 N の単位はブロック(1ブロックは、involution型暗号アルゴリズムの暗号

*する。

ステップ101) 初期値設定装置110を用いて最良偏差率の初期値を、

$\neg \text{BEST}_n = \text{BEST}_{n-1}$

と設定する。

【0040】ステップ102) 探索パターン抽出装置120(図4のフローチャート中の手続き名はExtract($n, \neg \text{BEST}_n$))を用いて、探索すべき探索パターン

10 Pattern _{i} ($P'_{11}, P'_{12}, \dots, P'_{1n}$) ($1 \leq i \leq \phi(n, \neg \text{BEST}_n)$)

を求め、探索パターン集合

【0041】

[数10]

[Pattern₁, Pattern₂, ..., Pattern _{$\phi(n, \neg \text{BEST}_n)$}]

化単位)である。 c は暗号アルゴリズムに依存する定数である。

20 【0047】最後に結果出力装置150により、上記平文情報量 N を結果ファイル170または、結果プリント180として出力する。次に、上記のフローチャートのステップ102における探索パターン抽出装置120が行う探索パターン抽出処理(手続きExtract($n, \neg \text{BEST}_n$))を以下に説明する。

【0048】図5は、本発明一実施例の探索パターン抽出装置の構成を示す。探索パターン抽出装置120は、探索パターン候補設定装置121、乗算器及び比較器122、探索計算量比較装置123、出力装置124、 f 関数の偏差率データ P' ファイル125、最良偏差率データ $V, < \text{BEST}_n$ ファイル126、探索パターン集合ファイル127より構成される。

30 【0049】図6は、本発明の一実施例の探索パターン抽出処理のフローチャートである。図6の処理を図5の構成と共に以下に説明する。

ステップ201) 探索パターン候補設定装置121を用いて、各段の f 関数の偏差率 P' を定めた探索パターンPattern _{i} [$P'_{11}, P'_{12}, \dots, P'_{1n}$]を設定する。

40 P'_{1j} ($1 \leq j \leq n$)のとり得る値は、暗号アルゴリズムの f 関数の構成に依存し、 f 関数を構成する個々の要素について線形近似を行うことで予め計算しておくことができる。例えば、DES暗号の場合、文献(松井充、「DES暗号の線形解読法(I)」、暗号と情報セキュリティシンポジウムSCIS93-3C, (Jan, 1993))に示されている。探索パターン候補設定装置121では、 $\neg \text{BEST}_n \leq P'_{1j} \leq 1/2$

を満たす P'_{1j} について全て調べればよい。

【0050】ステップ202) 探索パターン候補設定装置121で設定された探索パターンPattern _{i} に対して、乗算器及び比較器122を用いて、

13

$[p'_{i1}, p'_{i2}, \dots, p'_{in}] = \neg \text{BEST}_n$
を満たさない探索パターンは棄却し、ステップ201に移行する。

【0051】ステップ203) 乗算器及び比較器122を用いて、前述した条件1、

『条件1: 不要な探索パターンの削除

$1 \leq i \leq n, i+r-1 \leq n$ を満たす全ての i, r に対して以下の式を満たすこと。

$[q'_{i1}, q'_{i+1}, \dots, q'_{i+r-1}] \leq \text{BEST}_r$ 』

を満たすかをチェックする。満たさない探索パターンは棄却し、ステップ201に移行する。

【0052】ステップ204) 探索計算量比較装置123を用いて、前述した条件2、

『条件2: 重複探索の防止

探索パターン $(p'_{i1}, p'_{i2}, \dots, p'_{in})$ の探索に必要な計算量を $C(p'_{i1}, p'_{i2}, \dots, p'_{in})$ と定義*

①Procedure Search ($n, \text{Pattern}_i$) ... 手続き/探索

入力

n : 求める最良表現の段数

Pattern_{ni} : 探索パターン $(p'_{i1}, p'_{i2}, \dots, p'_{in})$

出力

BEST_n : n 段最良偏差率

②Procedure Round-1:

For each candidate for ΓO_1 and ΓI_1 , do the following:

† Let $p'_{i1} = p'_{i1}(\Gamma O_1, \Gamma I_1)$.

† If $p'_{i1} \neq p'_{i1}$, then try another candidate for ΓO_1 and ΓI_1 .

† Call Procedure Round-2.

$\text{BEST}_n = \neg \text{BEST}_n$

Print BEST_n .

Exit the program.

Procedure Round-2:

For each candidate for ΓO_2 and ΓI_2 , do the following:

† Let $p'_{i2} = p'_{i2}(\Gamma O_2, \Gamma I_2)$.

† If $p'_{i2} \neq p'_{i2}$, then try another candidate for ΓO_2 and ΓI_2 .

† Call Procedure Round-3.

Return to the upper procedure.

Procedure Round- r ($3 \leq r \leq n$)

For each candidate for ΓI_r , do the following:

† Let $\Gamma O_r = \Gamma O_{r-2} \odot \Gamma I_{r-1}$.

† Let $p'_{ir} = p'_{ir}(\Gamma O_r, \Gamma I_r)$.

† If $p'_{ir} \neq p'_{ir}$, then try another candidate for ΓI_r .

† If $r \neq n$ Call Procedure Round- $(r+1)$, else print

$\text{BEST}_n = [p_{i1}, p_{i2}, \dots, p_{in}]$

Return to the upper procedure.

次に、本発明を代表的なinvolution型暗号であるDESとFEAL-8に適用した結果について述べる。

【0055】【数値例1-DESへの適用】14段DE 50

14

*すると、以下の式を満たすこと。

$C(q'_{i1}, q'_{i2}, \dots, q'_{in}) \leq C(q'_{in}, q'_{n-1}, \dots, q'_{i1})$ 』

を満たすかをチェックする。満たさない探索パターンは棄却し、ステップ201に移行する。探索計算量の比較は、探索候補数を比較することで行う。

【0053】ステップ205) 上記の条件1、2を満たす探索パターン Pattern_i を出力装置124を介して探索パターン集合ファイル127に格納する。

10 ステップ206) 全ての探索パターンについて全てチェックしたら、処理を終了し、そうでなければ、ステップ201に移行する。

【0054】上記図4のステップ103において、最良表現探索装置130の手続き $\text{Search}(n, \text{Pattern}_i)$ のアルゴリズムを以下に示す。このアルゴリズムは、従来の方法を本発明に適合するように変更を加えただけであるので、フローチャートによる説明は省略する。

... 手続き/探索

Sの最良表現探索の結果、最良偏差率 BEST_{14} と最良表現は以下のように求められた。

最良偏差率: $BEST_{14} = 1.19 \times 2^{-21}$

最良表現: $P_L [7, 18, 24] \odot C_H [7, 18, 24, 29]$
 $\odot C_L [15] = K_2 [22] \odot K_3 [44] \odot K_4 [22]$
 $\odot K_6 [22] \odot K_7 [44] \odot K_8 [22] \odot K_{10} [22]$
 $\odot K_{11} [44] \odot K_{12} [22] \odot K_{14} [22]$

この最良表現から以下のDES (16段) の最良近似式 * めることができることが分かる。
 が求められ、 2^{43} ブロックの平文情報より暗号化鍵を求*

$P_H [7, 18, 24] \odot C_H [15] \odot C_L [7, 18, 24, 29]$
 $\odot F_1 (P_L, K_1) [7, 18, 24] \odot F_{16} (C_L, K_{16}) [15]$
 $= \odot K_3 [22] \odot K_4 [44] \odot K_5 [22] \odot K_7 [22] \odot K_8 [44]$
 $\odot K_9 [22] \odot K_{11} [22] \odot K_{12} [44] \odot K_{13} [22] \odot K_{15} [22]$

[数値例2-FEALへの適用] 7段FEALの最良表 ※のように求められた。以下のように、同一の最良偏差率
 現探索の結果、最良偏差率 $BEST_7$ と最良表現は以下※ $BEST_7$ を持つ最良表現が6種類存在する。

最良偏差率: $BEST_7 = 1.20 \times 2^{-8}$

最良表現 (1): $P_H [\Gamma\alpha] \odot P_L [\Gamma\beta] \odot C_H [\Gamma\alpha] \odot C_L [\Gamma\beta] =$
 $K_1 [\Gamma\delta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\delta]$

最良表現 (2): $P_H [\Gamma\varepsilon] \odot P_L [\Gamma\beta] \odot C_H [\Gamma\varepsilon] \odot C_L [\Gamma\beta] =$
 $K_1 [\Gamma\delta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\delta]$

最良表現 (3): $P_H [\Gamma\zeta] \odot P_L [\Gamma\eta] \odot C_H [\Gamma\zeta] \odot C_L [\Gamma\eta] =$
 $K_1 [\Gamma\theta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\theta]$

最良表現 (4): $P_H [\Gamma\iota] \odot P_L [\Gamma\eta] \odot C_H [\Gamma\iota] \odot C_L [\Gamma\eta] =$
 $K_1 [\Gamma\theta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\theta]$

最良表現 (5): $P_H [\Gamma\zeta] \odot P_L [\Gamma\eta] \odot C_H [\Gamma\varepsilon] \odot C_L [\Gamma\beta] =$
 $K_1 [\Gamma\theta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\delta]$

最良表現 (6): $P_H [\Gamma\iota] \odot P_L [\Gamma\eta] \odot C_H [\Gamma\alpha] \odot C_L [\Gamma\beta] =$
 $K_1 [\Gamma\theta] \odot K_2 [8] \odot K_3 [8, 10, 16]$
 $\odot K_5 [8, 10, 16] \odot K_6 [8] \odot K_7 [\Gamma\delta]$

上記の各 $\Gamma\alpha$ 、 $\Gamma\beta$ 、 $\Gamma\delta$ 、 $\Gamma\varepsilon$ 、 $\Gamma\zeta$ 、 $\Gamma\eta$ 、 $\Gamma\theta$ 、★【0056】

$\Gamma\iota$ は、以下の表に示す値を持つ。

★ 【表1】

$\Gamma\alpha$	2, 3, 4, 5, 6, 13, 14, 16, 20, 26, 28
$\Gamma\beta$	3, 4, 5, 6, 11, 12, 13, 14, 20, 28
$\Gamma\delta$	8, 10, 11, 12, 13, 14, 16, 20
$\Gamma\varepsilon$	2, 3, 4, 5, 6, 11, 13, 14, 16, 17, 20, 26, 28
$\Gamma\zeta$	2, 3, 4, 6, 11, 14, 17, 19, 20, 26, 27, 28
$\Gamma\eta$	3, 4, 6, 11, 12, 14, 19, 20, 27, 28
$\Gamma\theta$	8, 10, 11, 12, 14, 16, 19, 20
$\Gamma\iota$	2, 3, 4, 6, 14, 16, 19, 20, 26, 27, 28

【0057】但し、上記の表1の記号は次のビット位置を示す。

【0058】DESと同様にして、これらの最良表現からFEAL-8 (8段) の最近似式が求められる。この

最良近似式を用いて 2^{18} ブロックの平文情報より暗号化鍵を求められることが分かる。なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々、変更・応用が可能である。

【0059】

【発明の効果】本発明は、従来の方法に比べて暗号アルゴリズムの最良表現探索の効率化を図ったため、従来方式では、DES型のS-boxを持つ暗号アルゴリズム用として提案されているが、本発明では、探索に必要な計算量を減少させることにより、DESよりも探索計算量が多いFEAL等のinvolution型暗号へも実用的な時間内で適用可能となる。

【0060】ここで、従来より最良表現探索がどれだけ高速化されたかを例として、FEAL暗号に適用した場合*10

段数	本発明		従来法	
	探索候補数	実行時間	探索候補数	実行時間
3	304	0.00 秒	304	0.01秒
4	888	0.01 秒	59612	0.31秒
5	9.0×10^4	0.43 秒	4.8×10^6	21秒
6	5.1×10^7	230 秒	2.3×10^{11}	35時間
7		4.2 時間	2.1×10^{11}	* 1500日

【0062】

【図面の簡単な説明】

【図1】本発明の原理を説明するための図である。

【図2】本発明の原理構成図である。

【図3】本発明の一実施例の強度評価装置の構成図である。

【図4】本発明の一実施例の暗号アルゴリズムの強度評価方法の概要を示すフローチャートである。

【図5】本発明の一実施例の探索パターン抽出装置の構成図である。

【図6】本発明の一実施例の探索パターン抽出処理のフローチャートである。

【図7】一般のインボルーション(involution)型暗号アルゴリズムの説明図である。

【図8】マスク値の関係を示す図である。

【図9】3段DESの線形近似例を示す図である。

【図10】従来の探索パターンの例を示す図である。

【図11】従来の方法により探索されるパターンを示す

* 合について表2に示す。なお、最良表現探索のプログラムはC言語で記述し、Sun Microsystems社のワークステーションSRARC station10 model 30 (Super SPARC/36MHz, 31MIPS)を用いて実行時間を測定した。但し、*の付いたデータは探索候補数から見積もった実行時間である。FEALの7段の最良表現探索では約 8.6×10^3 倍高速化できることが予測される。

【0061】

【表2】

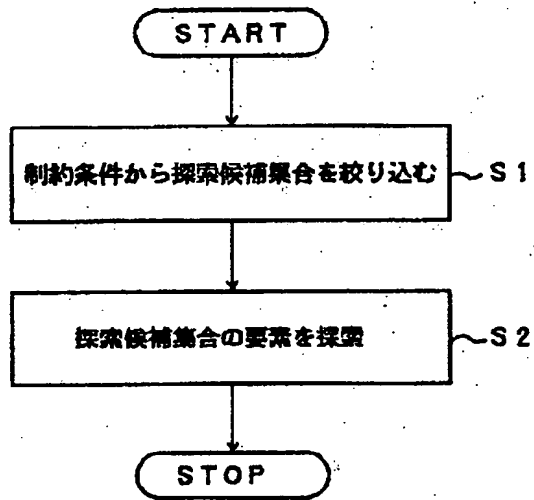
図である。

【符号の説明】

- 100 強度評価装置
- 110 初期値設定装置、初期値設定手段
- 120 探索パターン抽出装置、探索候補抽出手段
- 121 探索パターン候補設定装置
- 122 乗算器及び比較器
- 123 探索計算量比較装置
- 124 出力装置
- 30 125 f関数の偏差率データファイル
- 126 最良偏差率データファイル
- 127 探索パターン集合ファイル
- 130 最良表現探索装置、最良表現探索手段
- 140 必要平文情報量計算装置、平文情報算出手段
- 150 結果出力装置、出力手段
- 160 探索パターン集合ファイル
- 170 結果ファイル
- 180 結果プリント

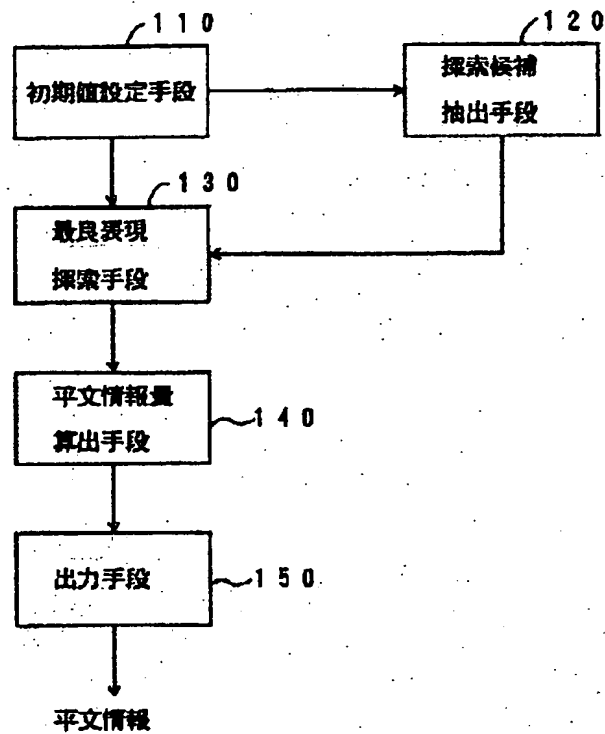
【図1】

本発明の原理構成図



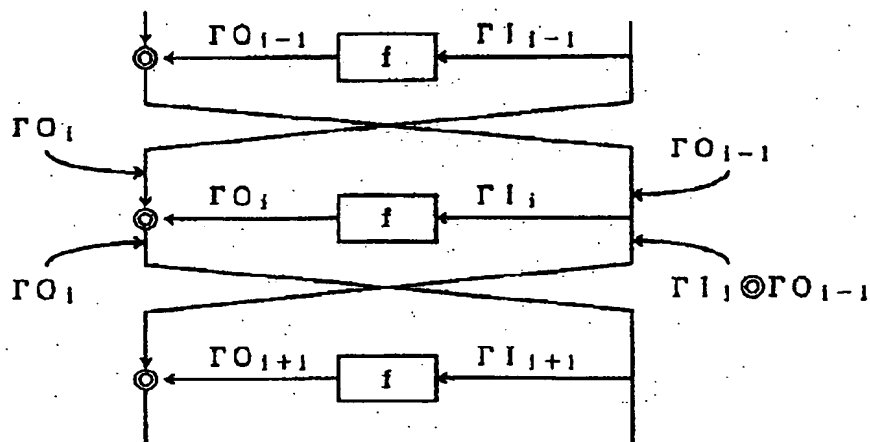
【図2】

本発明の原理構成図



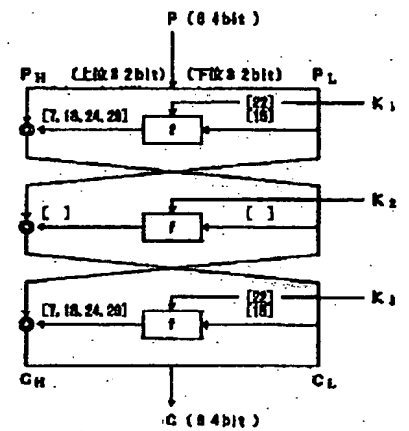
【図8】

マスク値の関係を示す図



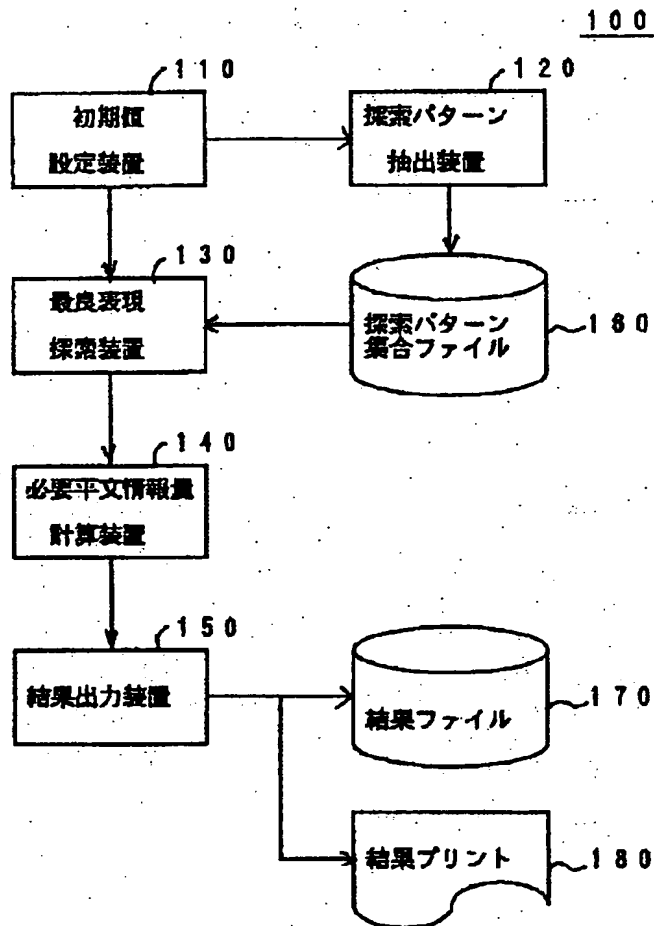
【図9】

1回DESの構成近似例を示す図



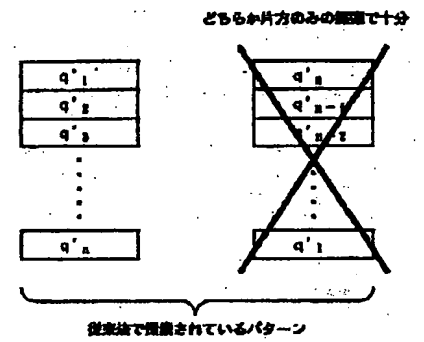
【図3】

本発明の一実施例の強度評価装置の構成図



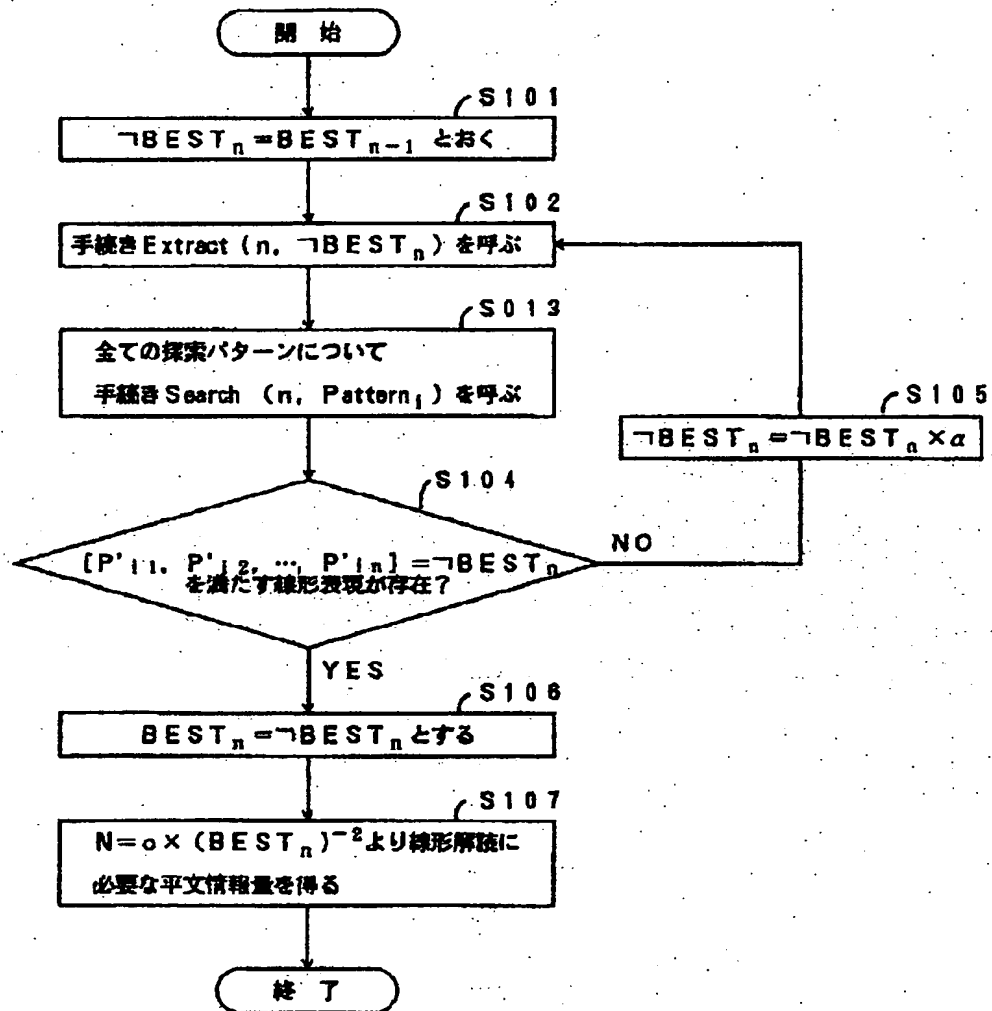
【図11】

従来の方法により検索されるパターンを示す図



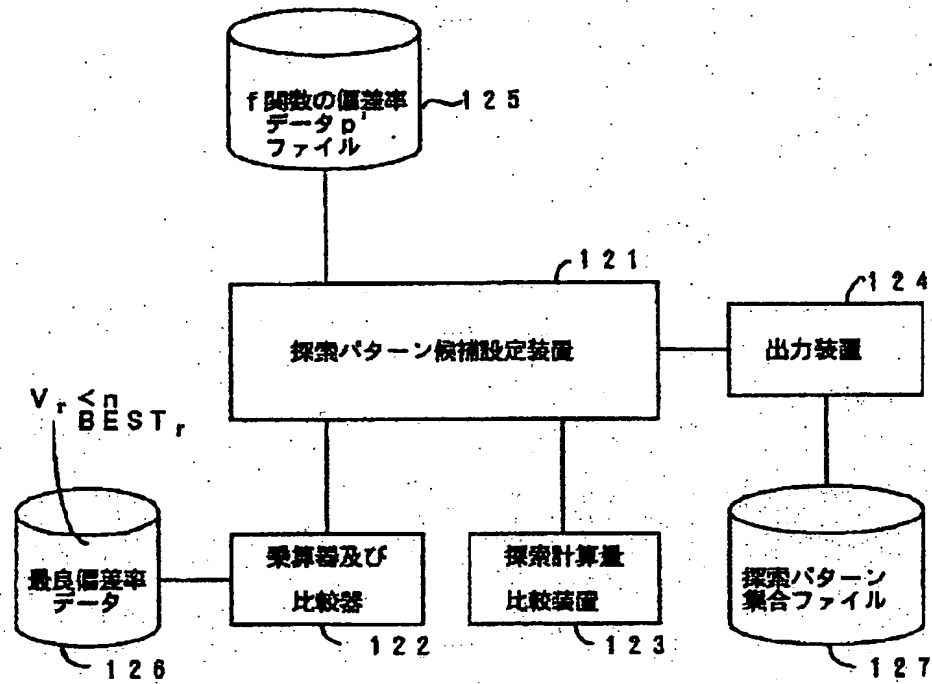
【図4】

本発明の一実施例の暗号アルゴリズムの強度評価方法の概要を示すフローチャート



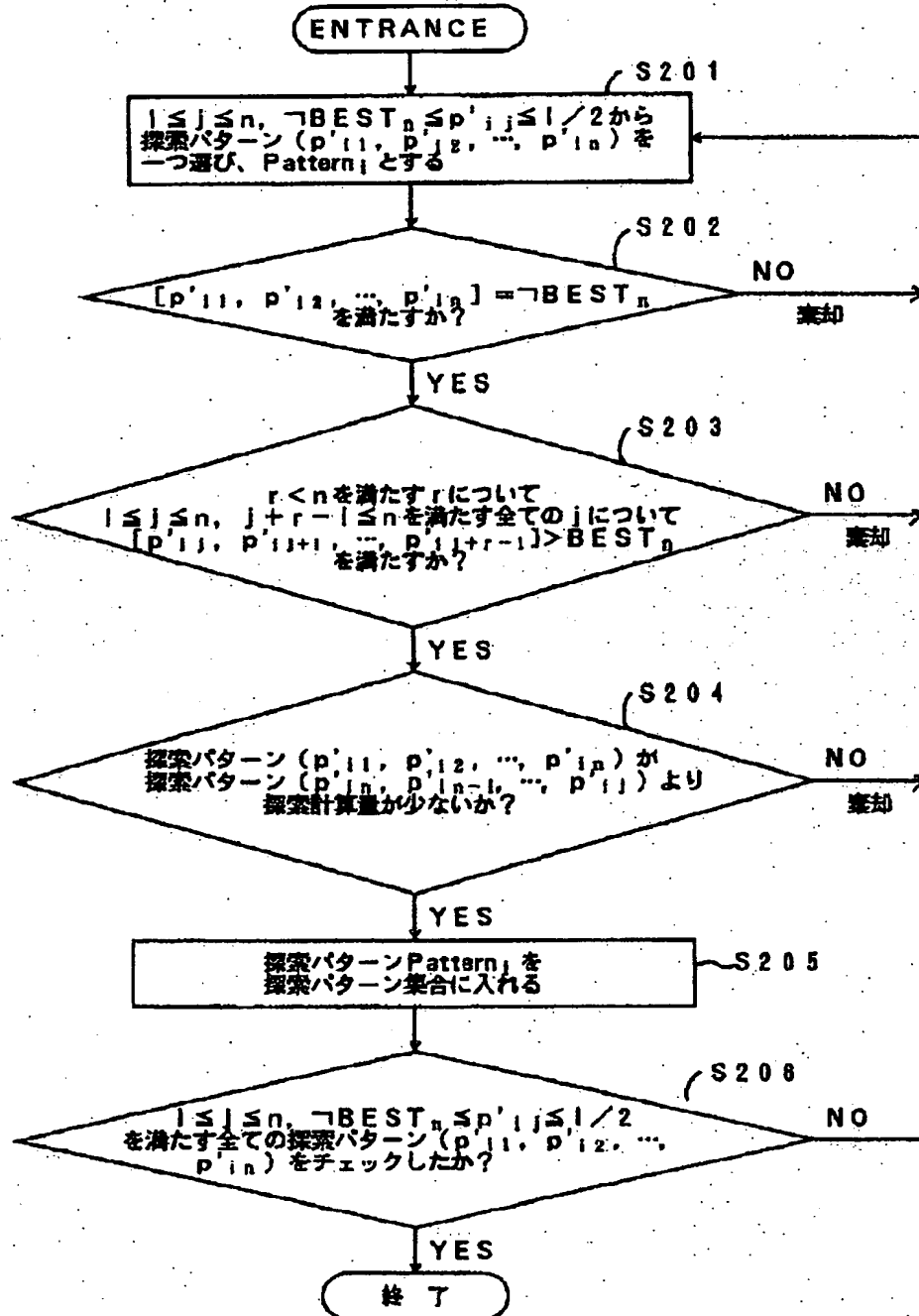
【図5】

本発明の一実施例の探索パターン抽出装置の構成図



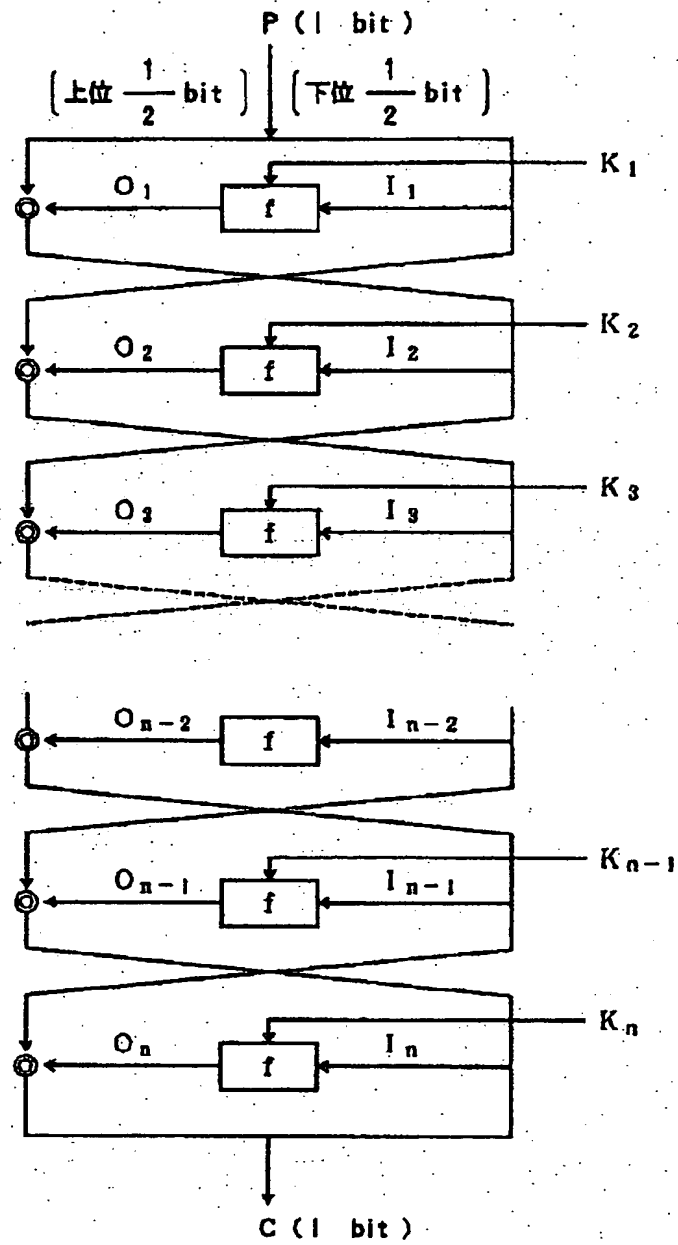
【図6】

本発明の一実施例の探索パターン抽出処理のフローチャート



【図7】

一般のインボルーション (involution) 型暗号アルゴリズムの説明図



【図10】

従来の探索パターンの例を示す図

